



# **TM-210, TM-270, TM-510, TM-560, TM-600, TM-800, TM-1000, TS-300, TS-700, TW-100 Administrator Manual**

**Version 5.0**



The RHUB TM-210 and TM-270 “6-in-1” web conferencing  
and TW-100 webinar appliances



The RHUB TM-510 and TM-560 “6-in-1” web conferencing  
and TS-300 remote support appliances



The RHUB TM-600, TM-800 and TM-1000 “6-in-1” web  
conferencing and TS-700 remote support appliances

RHUB Communications, Inc.  
4340 Stevens Creek Blvd.  
Suite 282  
San Jose, CA 95129  
[support@rhubcom.com](mailto:support@rhubcom.com)  
<http://www.rhubcom.com>

# Contents

<b>1. INSTALLATION &amp; REGISTRATION .....</b>	<b>3</b>
1.1. ACCESSING YOUR RHUB WEB CONFERENCING APPLIANCE.....	3
1.2. REGISTERING YOUR RHUB WEB CONFERENCING APPLIANCE .....	5
<b>2. CONFIGURING THE RHUB WEB CONFERENCING APPLIANCE .....</b>	<b>6</b>
2.1. CONFIGURE SERVER IP SETTINGS .....	8
2.2. SYSTEM SETTINGS .....	10
2.3. MANAGING YOUR SSL CERTIFICATE .....	12
2.4. SCHEDULED MEETINGS AND ACTIVE MEETINGS.....	14
2.5. RESTORE OR TRANSFER EXISTING, EXPIRED OR DELETED MEETINGS .....	15
2.6. CUSTOMIZING THE MEETING START AND PROMOTION PAGES .....	15
2.7. WEBINAR REGISTRATION .....	18
2.8. INTEGRATION .....	20
2.9. INTEGRATION WITH LDAP FOR USER AUTHENTICATION .....	20
<b>3. CONFIGURING THE FIREWALL .....</b>	<b>22</b>
3.1. BEHIND FIREWALL AND ACCESSIBLE BY USERS OUTSIDE FIREWALL .....	22
3.2. OUTSIDE THE FIREWALL.....	23
3.3. BEHIND FIREWALL AND NOT ACCESSIBLE BY USERS OUTSIDE FIREWALL .....	24
<b>4. MANAGE USERS .....</b>	<b>25</b>
4.1. USER GROUPS .....	26
<b>5. START MEETINGS.....</b>	<b>28</b>
<b>6. REPORTING.....</b>	<b>30</b>
<b>7. RESET APPLIANCE .....</b>	<b>31</b>
<b>8. LICENSE UPGRADES: ADDITIONAL MEETING ROOMS AND USERS...</b>	<b>32</b>
<b>SUPPORT CONTACT .....</b>	<b>33</b>

# 1. Installation & Registration

---

The Web conferencing server package includes:

- TM-200, TM-260, TS-300, TM-510, TM-560, TM-600, TM-800, TM-1000, or TS-700 appliance (or server)
- Analog console cable
- Power cord. Power brick (for TM-200, TS-300, TM-260, TM-250E, and TM-550 only)

## 1.1. Accessing your RHUB Web Conferencing Appliance

There are two ways to access the TM-200 and TM-260 appliances: by using plug-and-play or by using a direct cable connect. To access the TM-510, TM-560, TM-600, TM-800, TM-1000, TS-300 and TS-700 appliances, use plug-and-play. In all cases, an Internet browser needs to be used to access and configure the server.

### I. Plug-and-Play

This method requires that you have:

- A DHCP server on your network
- A computer with Microsoft Windows (2000, XP, Vista, Windows 7, or Windows 8)

It is important to follow the instructions below to start the server for initial setup:

1. Connect the server with an Ethernet cable (not a crossover cable) to your network
2. Plug in the power cord to automatically power on the server
3. Wait for the ready light to turn green. This usually takes about 30 seconds.

Open a browser on your computer and type "<http://myonlinemeeting>". The following page should appear:

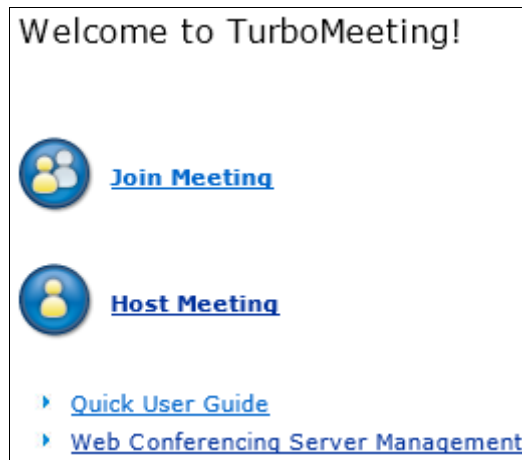


Figure 1.1 Home Page

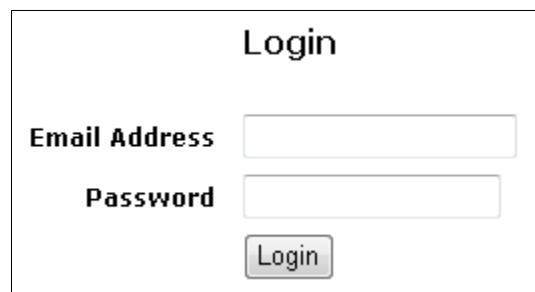
If the page does not display and you are familiar with your router, check the IP address your router has assigned to the RHUB appliance, which is named "myonlinemeeting". Then input the IP address in your browser's address bar and you will be able to access the RHUB appliance.

If the page does not display and you are not familiar with your router, go to the following initial startup method.

## II. Local Access

For the TM-600, TM-800, TM-1000, and TS-700 appliances only, if you fail to access the appliance by the above method, do the following:

- Plug in your keyboard, mouse and monitor to the appliance
- Power on the appliance
- Wait for 1 minute
- Type "**turbomeeting**" as the Username and "**password**" as the Password
- Wait for up to a couple of minutes and you will be connected to the Fedora desktop.
- Open a browser by clicking the browser icon on the top banner
- This will take you to the TurboMeeting web login page (Figure 1.2)
- Follow the sections below to configure the appliance using the browser.



The image shows a web login form titled "Login". It contains two input fields: "Email Address" and "Password". Below the "Password" field is a "Login" button.

Figure 1.2. Login

For the TM-250-E, TM-550, TM-510 and TM-560 appliances only, if you fail to access the appliance by Plug-and-Play, do the following:

- Plug a serial cable between the appliance and a computer
- Power on the appliance
- Wait for 1 minute
- Use HyperTerminal or the open source TeraTerm program
- Type "**admin**" as the Username and "**password**" as the Password
- Type "ifconfig" to determine the IP address (inet addr) of the appliance
- Follow the sections below to configure the appliance using the browser.

## III. Direct-Cable Connection

The direct-cable connection method is only used for the TM-200 and TM-260. Before you use this method, configure your computer (in any operating system) with the following IP setting:

- IP Address: 192.168.1.100
- Subnet Mask: 255.255.255.0

Next, do the following:

- Disconnect your computer from any network including the wireless
- Power on the TM-200 or TM-260 (as described above)
- Wait for the ready light to turn green. This usually takes about 90 seconds
- Connect the TM-200 or TM-260 to your computer using the included crossover-cable or any Internet cable
- On your computer, open a browser and in the address bar type <http://192.168.1.192>. The home page (Figure 1.1) should display.
- Because your appliance is not connected to the Internet, when you click the link "Web Conferencing Server Management", the registration page (Figure 1.3) will not display. To bypass the registration page, type <http://192.168.1.192/as/wapi/login?b=y>.

Once you have accessed the meeting server, you are ready to configure the server. Do not disconnect your computer from the meeting server before you complete the configuration described in the next section. After the configuration, connect the TM-200 or TM-260 to your network using a regular Ethernet cable (which is not included).

Note that after you change the system IP settings, the web page will hang. You will need to use the new IP address to access the appliance.

## 1.2 Registering your RHUB Web Conferencing Appliance

When you receive your RHUB appliance, you have to register in order to receive software updates and technical support. To register your appliance, access the meeting server home page (Figure 1.1), and click the "Web Conferencing Server Management" link. The Registration Page (Figure 1.3) appears. If you are using the direct-cable connection method to access your appliance (Section 1.1, Part III), type <http://192.168.1.192/as/wapi/login?b=y> to bypass the registration page since the appliance is not connected to the internet yet.

It is important to specify an email address that will last a long time to insure that you receive important notices such as product release notes from the manufacturer.

### Register and Activate Your Appliance

Registration is required for support and warranty purposes. An accurate long-term email address is most critical to receive important notices such as release notes from the manufacturer. Your contact information is strictly protected.

If you don't see the registration form below, check your Internet connection and make sure your DNS setting is correct.

**First Name**  \* (Required)

**Last Name**  \*

**Email**  \* (The email address needs to be accurate and stable)

**Phone**  \*

**Organization**  \*

**URL**

Figure 1.3 Registration Page

## 2. Configuring the RHUB Web Conferencing Appliance

---

After you access the meeting server home page (Figure 1.1), click the “Web Conferencing Server Management” link. If your RHUB appliance is new, you will have to submit

- **admin** for the Email field
- **password** for the Password field

To change the default administrator account, you use “Manage Users” (see Section 4) to change the default email and password to your choice.



The image shows a login form titled "Login". It contains two input fields: "Email Address" and "Password". Below the "Password" field is a "Login" button.

Login	
Email Address	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	

Figure 2.1 Login Page

After login, the **System Management** home page is displayed. The System Management Navigation frame is shown in Figure 2.2:

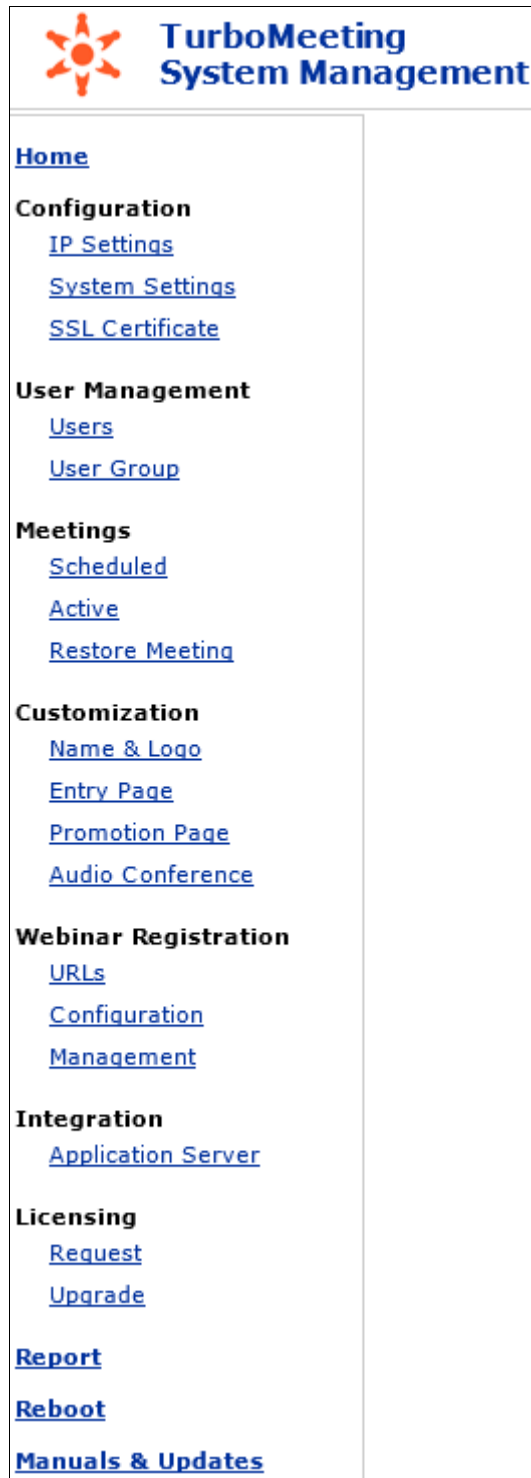


Figure 2.2 Management Home Frame

## 2.1. Configure Server IP Settings

In the left frame of the System Management page, under Configuration click the [IP Settings](#) link. Figure 2.3 is displayed:

### Configure Server IP Settings

**Public IP Address:** ☒ Public IP address or domain name  
 (e.g., 168.87.66.196, webmeeting.acme.com)

☐ Dynamic DNS host name if you don't have a static public IP address  
[Click this link for instructions to setup a dynamic DNS host name](#)

**Host Name:**  (e.g., meeting.homedns.org)

**User Name:**

**Password :**

**Retype Password :**

☐ No public IP address. This server is used only by internal users.

**Authorized Public IP's to Join Internal Meetings**   
(Multiple IP's are separated by commas, e.g., 29.12.21.9, 122.21.23.190)

<b>Current IP Settings</b> (After each reset, the current IP settings are acquired by DHCP. They are temporary.)	IP Address:	192.168.1.122
	Subnet mask:	255.255.255.0
	Default Gateway:	192.168.1.1
	DNS 1:	8.8.8.8
	DNS 2:	8.8.4.4

<b>Permanent IP Settings</b> (After each reset, you need to submit this form once in order to enable this permanent IP settings, which are required.)	IP Address	<input type="text" value="192.168.1.122"/>
	Subnet mask	<input type="text" value="255.255.255.0"/>
	Default Gateway	<input type="text" value="192.168.1.1"/>
	Preferred DNS server	<input type="text" value="8.8.8.8"/>
	Alternate DNS server	<input type="text" value="8.8.4.4"/>

Figure 2.3 Configure Server IP Settings

Note that if you change the IP settings and submit the changes, your browser may hang because the IP is changed. You should use the updated IP to access the appliance.



The following describes the fields in Figure 2.3.

- **Public IP Address**

In order for users outside your LAN to host or join meetings, you have to assign a public IP address. If you don't have a fixed public IP address, you can go to <http://www.dyndns.com> to set up a domain name and copy the domain information and your DynDNS user account information to the meeting server configuration page. After that, you can always access your RHUB appliance by the domain name you set at DynDNS.

Note that RHUB offers the DynDNS client as a convenience to our customers. RHUB is in no way affiliated with DynDNS or responsible for their service. Any fees that you may incur with DynDNS are between you and DynDNS and have nothing to do with RHUB.

- **Authorized Public IP's to Join Internal Meetings**

If you have branch offices outside your LAN and you don't have a VPN, use this setting to allow employees from those branch offices to join an internal secured meeting hosted in your LAN.

- **Current IP Settings**

These are the IP addresses that the meeting server has currently.

- **Permanent IP Settings**

The Permanent IP Settings refer to the desired IP settings you want your meeting server to have. The permanent IP address can be the same as the "Public IP Address" or different from the "Public IP Address". If the permanent IP is a local IP address, it will be different from the public IP address. In such a case, you will need to do port forwarding on your firewall router to forward TCP traffic from the ports (80 and 443) and TCP and UDP traffic from the port (8889) at the public IP address to the corresponding ports at the permanent IP address. See the next section for details.

Carefully check that the DNS settings are correct. Correct DNS settings are needed to allow the meeting server appliance to connect to the RHUB Communications' release servers so firmware updates can be applied. Correct DNS settings are also needed to allow updated audio conference numbers to be sent to your meeting server appliance.

Note that after you change the permanent IP settings, the web page will hang because the server IP address has been changed. You will need to use the new IP address to access the appliance.

If you make a mistake in configuration, you need to reset the appliance. See Section 7 for details.

## 2.2. System Settings

In the left frame of the System Management page, under Configuration click the [System Settings](#) link. Figure 2.4 is displayed.

**System Settings**

**Language** English

**Time Zone** (GMT-08:00) Pacific Time (US & Canada)

**Time & Date** 18 hour 07 minute 10/03/2011 (Don't change the date format)

**Date Format:** (used to display reports, etc.) YYYY.DD.MM (e.g., 12/31/2010 is in format of MM/DD/YYYY)

**Max free speakers in a VoIP session** 5 (Note that the VoIP bandwidth consumption will dramatically increase as more free speakers are allowed. Additional participants will use a push-to-talk function to join VoIP-based audio conferencing.)

**Max Webcam Height:** 240 pixels (Larger height will increase traffic load. To turn on the max webcam height, click the maximum icon on the webcam dialog.)

**Webcam Image Quality:** Medium (Higher quality image will increase traffic load)

☒ Enable VoIP audio conferencing

☒ Allow attendees to record

☒ Enable multipoint video conferencing

☐ Access this server only via SSL (this will reduce system performance)

☒ Use SSL to manage the server web pages

☐ Enable auto update of system (recommended)

(only if auto-update is disabled)

Figure 2.4 System Settings

The following describes the fields in Figure 2.4.

- **Language**

The language for the TurboMeeting System Management UI can be changed to English, Chinese (Simplified), Chinese (Traditional), Japanese, Spanish, French or Portuguese.

- **Time Zone, Time & Date, and Date Format**

Set the correct time zone, time and date, and date format for the RHUB appliance.

- **Max free speakers in a VoIP session**

Set the maximum number of free speakers in a VoIP session before attendees must use the Push-to-Talk button in order to be heard in a meeting. 5 is the default maximum number of free speakers. The presenter and the controller are always free to talk. All attendees should use good quality headsets, such as those from Plantronics, to avoid

echo and background noise. Internet traffic can grow quickly if too many free speakers are allowed on your appliance at once.

- **Max Webcam Height**

Change the Maximized Webcam height when the host clicks the Webcam's Maximize button. The default maximum height is 240 pixels. Other choices include 320 pixels, 480 pixels and 560 pixels. Webcams use 10 times as much bandwidth in a meeting compared to other features; and a "560" pixel setting will use twice as much bandwidth as the "240" pixel setting.

- **Webcam Image Quality**

Set the image quality of webcams. The possible settings are Low, Low to Medium, Medium, Medium to High, and High. The "High" setting can use twice as much bandwidth as the "Low" setting.

- **Enable VoIP audio conferencing**

Disable or enable VoIP audio conferencing for your RHUB appliance.

- **Allow attendees to record**

This setting determines whether any attendees are allowed to record during a meeting.

- **Enable multipoint video conferencing**

This setting determines if multipoint video conferencing is enabled for this RHUB appliance. Multipoint video conferencing allows up to four meeting participants to show their webcams.

- **Access this server only via SSL**

By default, screen images during a meeting are transmitted with RHUB proprietary 256-bit encryption for efficiency. However, you can use SSL for encryption by enabling the **Access this server only via SSL** option. See the section **Manage Your SSL Certificate** about how to upload your own SSL Certificate.

- **Use SSL to manage the server web pages**

This setting determines if SSL is always used when displaying the TurboMeeting System Management web pages.

- **Enable auto update of system**

The RHUB appliance retrieves software updates automatically if this is enabled. This is done at 3 AM for the time set on the appliance. Updates typically happen twice per year.

- **Update System Now**

This feature retrieves updated RHUB appliance software from the RHUB web site.

## 2.3. Managing Your SSL Certificate

In the left frame of the System Management page, under Configuration click the [SSL Certificate](#) link. Step 1 of setting up an SSL certificate is displayed as in Figure 2.5.

**Step 1: Generate Your CSR** (Certificate Signing Request)  
**Alert!** Generating a CSR will revoke your existing SSL certificate if you have uploaded one in the system.  
**Common Name:**  \* (Required) (e.g., webmeeting.acme.com)  
**Organization Name:**  \* (e.g., Acme, Inc.)  
**State:**  \* (e.g., California. Use the full name)  
**City:**  \* (e.g., San Jose)  
**Country:**  

Figure 2.5 Setting up an SSL Certificate, step 1

The following describes the fields in Figure 2.5.

- **Common Name**

This is the domain name for your RHUB appliance. This must match the domain name you specify in your SSL certificate.

- **Organization Name**

This is the Organization Name you specify in your SSL certificate.

- **State, City and Country**

This is the State, City, and Country that you specify in your SSL certificate.

Next, obtain an SSL certificate as shown in Step 2 (Figure 2.6). For the SSL certificate, specify the same Common Name, Organization, State, City and Country that you specified in Step 1.

**Step 2: Purchase Your SSL Certificate**

You may go to <http://www.godaddy.com> and purchase an affordable SSL certificate with the CSR you just created. When downloading your certificate, select "Apache " as the "Server Type".

Figure 2.6 Setting up an SSL Certificate, step 2

Locate your SSL Certificate file and your CA Root Certificate file (which may be called a "bundled root"). Sometimes your SSL provider may bundle these two into the same file. Using Microsoft WordPad, copy and paste the contents of these files into the files shown in step 3 (Figure 2.7).

### Step 3: Upload SSL Certificates

(Use Microsoft WordPad to open the certificates to copy and paste. Don't use Notepad as it does not properly handle Unix newlines in the file.)

**Your SSL Certificate:**  
(The file name has a ".crt" extension)

```

-----BEGIN CERTIFICATE-----
MIIEhjCCA26gAwIBAgIQUKIGSk83/kNpSHqWZ/9dJzANBgkqhkiG9w0
BAQUFADBv
MQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRKVHJ1c3QgPACkErSkBgN
VBAsTHUFk
ZFRydXNOIEV4dGVybmAtTHLETICSZXR3b3JrMSIwIAYDVQQDEEx1BZGR
UcnVzdCBF
(.....)
vm9nu/9iVzmdDE2yKmE9HZzvmncgoC/uGnKdsJ2/eBMnBwpgEZP1Dy7
J72skg/6b
kLRLaIHQwvrgPw==
-----END CERTIFICATE-----

```

**CA Root Certificate:**  
(The file name has a ".ca-bundle" extension)

```

#####
#####
##  ca-bundle.txt -- Bundle of CA Root Certificates
##
##  Original Date: Thu Mar  2 11:42:76 CET 2008
(.....)
81:e7:11:50:db:3e:e2:d7:10:2e:6a:15:7f:b7:d4:a3:62:b2:
89:69:61:57:c6:7f:8e:9e:d4:24:7a:f3:a1:43:5f:a0:7a:89:
dc:59:cd:7d:d7:75:a7:bc:53:d5:47:35:c6:31:30:20:9f:9b:
ba:b5:83:e6:89:55:01:4d:91:3b:d6:89:35:87:3c:83:6b:7a:
29:82:d4:4b:d4:e6:16:74:b0:01:10:ab:69:06:14:37:7b:f7:
66:30:3a:c5

```

Figure 2.7 Setting up an SSL Certificate, step 3

Test your SSL Certificate as described in step 4 (Figure 2.8).

### Step 4: Test Your SSL Certificate

Reboot this system. After reboot, open a browser and type <https://your-domain-name> to test your SSL certificate. If you see a security alert and the manufacturer default certificate, check the following:

- You generated several CSRs and did not use the latest one to purchase your SSL.
- You are using a CA or a type of certificate that this system does not support.

Other issues regarding your certificate would be explained by your browser.

Figure 2.8 Setting up an SSL Certificate, step 4

Note that the RHUB appliance does not accept wildcard certificates.

## 2.4. Scheduled Meetings and Active Meetings

In the left frame of the System Management page, under Meetings click the [Scheduled](#) link. This feature shows you the list of scheduled meetings for your RHUB appliance. The provided URLs show all of the public meetings and provide a link for how to join the meeting.

List of Scheduled Meetings						
<b>► The URL to publish the scheduled public meetings in HTML:</b> <a href="http://qa2.rhubcom.com/as/wapi/list_public_scheduled?cuid=HxNeYy4GHCp3WXtEekwYOjk0XAsKSQEQWUyBwMFCq4z">http://qa2.rhubcom.com/as/wapi/list_public_scheduled?cuid=HxNeYy4GHCp3WXtEekwYOjk0XAsKSQEQWUyBwMFCq4z</a>						
<b>► The URL to publish the scheduled public meetings in XML:</b> <a href="http://qa2.rhubcom.com/as/wapi/list_public_scheduled?is_xml=Y&amp;cuid=HxNeYy4GHCp3WXtEekwYOjk0XAsKSQEQWUyBwMFCq4z">http://qa2.rhubcom.com/as/wapi/list_public_scheduled?is_xml=Y&amp;cuid=HxNeYy4GHCp3WXtEekwYOjk0XAsKSQEQWUyBwMFCq4z</a>						
<b>► List of Scheduled Meetings:</b>						
Meeting ID	Meeting Subject	Start Time	Time Zone	Host Name	Host Email	Host Phone
14704084	Interactive	Recurring	(GMT-08:00) Pacific Time (US & Canada)	John Doe	john@doe.com	242-424-2424
18860313	Seminar	Recurring	(GMT-08:00) Pacific Time (US & Canada)	John Doe	john@doe.com	242-424-2424

Figure 2.9 List of scheduled meetings

In the left frame of the System Management page, under Meetings click the [Active](#) link. This feature shows you the list of active meetings for your RHUB appliance. As the administrator, you can stop an Active meeting by clicking the [Stop](#) link as shown in Figure 2.10.

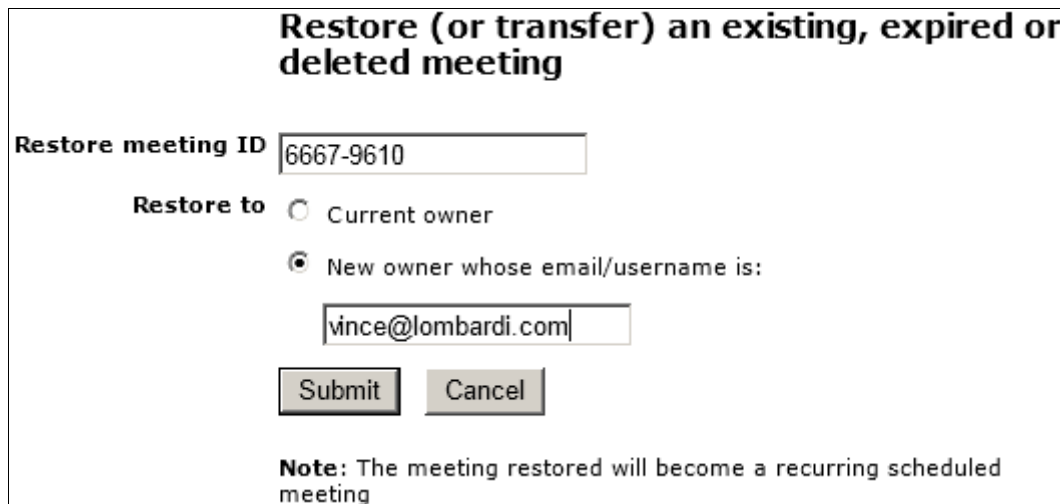
List of active meetings								
Meeting ID	Meeting Subject	Host Name	Meeting Type	Host Phone	Last Connect Time	Number Of Users	Host IP	Action
14704084	Interactive	John Doe john@doe.com	Interactive	242-424-2424	04/02/2013 16:56	2	74.93.8.30	<a href="#">Stop</a>
18860313	Seminar	John Doe john@doe.com	Seminar	242-424-2424	04/02/2013 15:53	18	74.93.8.30	<a href="#">Stop</a>

Figure 2.10 List of active meetings

## 2.5. Restore or Transfer Existing, Expired or Deleted Meetings

In the left frame of the System Management page, under Meetings click the [Restore Meeting](#) link. This feature allows you to restore a meeting that has expired or was deleted; and it allows you to transfer a meeting to another user, which is helpful if the original host of the meeting is unavailable.

To restore a meeting to its original owner, enter the meeting ID and select Restore to "Current owner"; click "Submit". To transfer a meeting to a new owner, enter the meeting ID, select Restore to "New owner whose email/username is" and specify the email id or user name; click "Submit".



**Restore (or transfer) an existing, expired or deleted meeting**

Restore meeting ID

Restore to ☐ Current owner

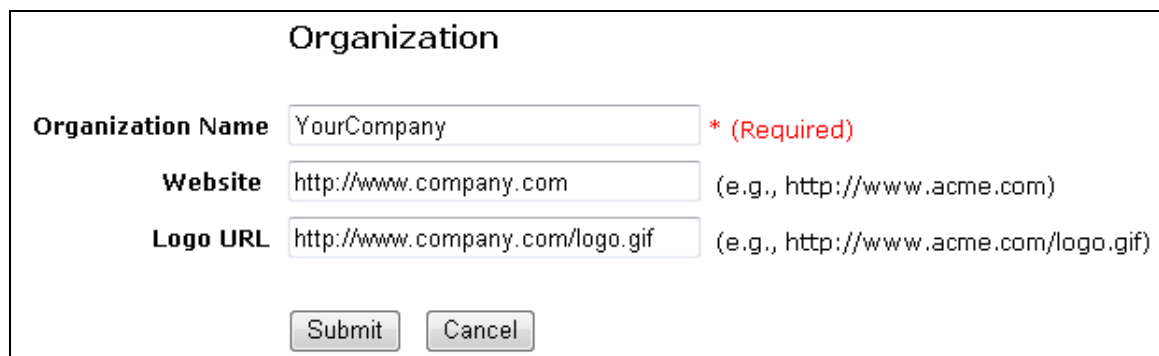
☒ New owner whose email/username is:

**Note:** The meeting restored will become a recurring scheduled meeting

Figure 2.11 List of scheduled meetings

## 2.6. Customizing the Meeting Start and Promotion Pages

In the left frame of the System Management page, under Customization click the [Name & Logo](#) link. This feature allows the Administrator to use show your company's name and logo on the standard meeting home page.



**Organization**

Organization Name  \* (Required)

Website  (e.g., http://www.acme.com)

Logo URL  (e.g., http://www.acme.com/logo.gif)

Figure 2.12 Change the name and logo on standard meeting home page

In the left frame of the System Management page, under Customization click the [Entry Page](#) link. This feature allows the Administrator to use a different home page as the standard meeting home page.

### Use My Page as the System Home Page

**Alert!** Before you start to use your own home page, carefully prepare the following:

- Note the URL below for accessing the system management pages. Keep it for reference.  
<http://192.168.1.122/as/wapi/login>
- Note the Host and Join Meeting URLs and the download URL on the default system home page. You may need those URLs on your own system home page.
- To change back to the default system home page, just leave your system home page URL empty.

Further instructions on how to customize this system can be found in the support section of the RHUB website:  
<http://www.rhubcom.com>.

**My system home page URL:**

(e.g., <http://www.acme.com/meeting.html>)

Figure 2.13 Use a new page for the meeting home page

The system home page specified in Figure 2.13 should contain ways for users to host and join meetings. There are two ways for users to host and join meetings:

1. click URLs (or buttons associated with the URLs) on your page
2. submit forms on your page

Using URLs is the easiest way for customization. Using forms gives you a better control of customization. In the following examples, substitute for `yourMeetingServerAddress` the host name (e.g. `webmeeting.company.com`) for your RHUB appliance.

Here is the URL that is used to host a meeting:

```
http://yourMeetingServerAddress/as/wapi/goto_downloader?role=host
```

Here is the URL that is used to join a meeting:

```
http://yourMeetingServerAddress/as/wapi/goto_downloader?role=attendee
```

Here is the HTML code used to allow users to host a meeting:

```
<form action="http://yourMeetingServerAddress/as/wapi/goto_downloader"
      method="post">
  <input type="hidden" name="role" value="host">
  Email Address:
    <input type="text" name="email" value="">
  Password:
    <input type="password" name="user_password" value="">
    <input type="submit" name="submit" value="Host Meeting">
</form>
```



Here is the HTML code used to allow users to join a meeting:

```
<form action="http://yourMeetingServerAddress/as/wapi/goto_downloader"
method="post">
  <input type="hidden" name="role" value="attendee">
  Meeting ID:
    <input type="text" name="meeting_id" value="">
  Meeting Password:
    <input type="password" name="password" value="">
  Your Name:
    <input type="text" name="name" value="">
  <input type="submit" name="submit" value="Join Meeting">
</form>
```

In the left frame of the System Management page, under Customization click the [Promotion Page](#) link. This allows the Administrator to change the web page that meeting attendees see when a meeting ends. The web page can be used to solicit feedback, sell products or services, or display your organization's home page.

**Promotional URL, presented to attendees when meetings end**  
 (e.g., http://www.acme.com)

Figure 2.14 Change default promotion page

In the left frame of the System Management page, under Customization click the [Audio Conference](#) link. This allows the Administrator to change the telephone number used for audio conferencing.

**Audio Conferencing Options:**  
  
☐ None  
☐ My audio conferencing number:  
  
**Attendee Access Code:**  
  
  
☐ Use Meeting ID as the audio conference access code  
☒ RHUB integrated free audio conferencing service allowing the use of regular phones & computer microphones in the same conference.

Figure 2.15 Change audio conference phone number

## 2.7. Webinar Registration

In the left frame of the System Management page, under Webinar Registration click the [Configuration](#) link. This feature allows the Administrator to setup a registration page for all of your webinars. Figure 2.16 shows the fields that can be customized for this registration page:

### Configure Webinar Registration

**Headline**

**Welcome message**  

Join us for a 1 hour webinar from on of the greatest minds of our time.

The welcome message is displayed just below the headline. You can leave the welcome message empty.

**Fields to be filled in by users**

☒ Name  
☒ Email  
☒ Job Title  
☒ Phone  
☒ Organization Name  
☒ Address  
☐ This is a customized field with the following field name:

**Confirmation page after registration**

☒ Use the default page provided by the system with the following message:  

You are registered!

  
☐ Use the following URL:

**Display all coming webinars within the following days:**

**Note:** You can build your own registration page and publish it to your own website by using the sample registration page:

[Get the sample registration page](#)

Figure 2.16 Registration page for all webinars

In the left frame of the System Management page, under Webinar Registration click the [Management](#) link. This feature allows the Administrator to list, create, edit and disable upcoming webinars. As shown in Figure 2.17:

Webinar Management						
From 05/28/2010		Retrieve Webinars		New Webinar		
ID	Subject	Host	Start Time	Status	Registration	Action
3	Learn how to become 'The Decider'	G W	05/28/2010 10:00	Active	View (0)	<a href="#">Edit</a>   <a href="#">Disable</a>
4	Never underestimate the power of the internets	G W	06/01/2010 10:00	Active	View (0)	<a href="#">Edit</a>   <a href="#">Disable</a>
5	Is our children learning?	G W	06/02/2010 10:00	Active	View (0)	<a href="#">Edit</a>   <a href="#">Disable</a>

Figure 2.17 List, Create, Edit and Disable Webinars

The resulting registration page for webinar attendees will look what is shown in Figure 2.18:

### YourCompany's Webinar Registration

Join us for a 1 hour webinar from one of the greatest minds of our time.

Name

Job Title

Email

Phone

Organization

Address

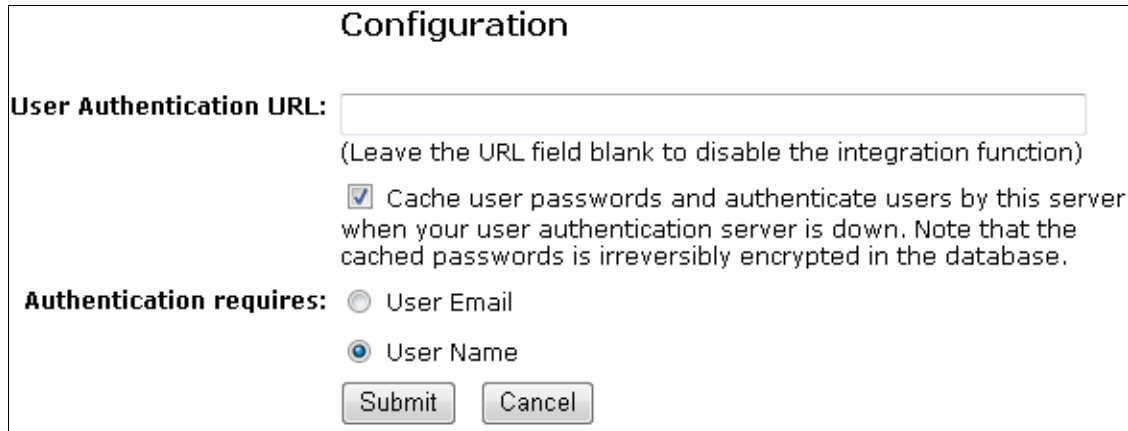
Select a webinar to attend

☐ [Learn how to become 'The Decider'](#)  
05/28/2010 10:00 Eastern Time
   
  
☐ [Never underestimate the power of the internets](#)  
06/01/2010 10:00 Eastern Time
   
  
☐ [Is our children learning?](#)  
06/02/2010 10:00 Eastern Time

Figure 2.18 Webinar Registration page for Attendees

## 2.8. Integration

In the left frame of the System Management page, under Integration click the [Application Server](#) link. This feature allows the Administrator to use their own authentication server, such as a CRM system, for user authentication.



The screenshot shows a web form titled "Configuration". It has a section for "User Authentication URL:" with a text input field. Below the field is a note: "(Leave the URL field blank to disable the integration function)". There is a checked checkbox labeled "Cache user passwords and authenticate users by this server when your user authentication server is down. Note that the cached passwords is irreversibly encrypted in the database." Below this is a section "Authentication requires:" with two radio buttons: "User Email" (unselected) and "User Name" (selected). At the bottom are "Submit" and "Cancel" buttons.

Figure 2.19 Integration with your server for user authentication

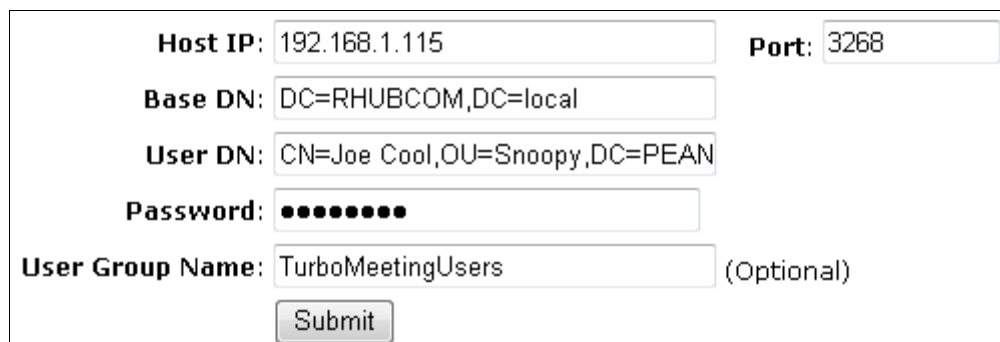
For more details on how to integrate with an authentication server:

1. Go to <http://www.rhubcom.com>
2. Click the "Support" link
3. Click the [Integration](#) link

## 2.9. Integration with LDAP for User Authentication

LDAP Integration works on all appliances. The LDAP feature is enabled for free on the TM-600, TM-800, TM-1000, and TS-700 appliances. Login to your RHUB appliance and enter the management page shown in Figure 2.2. Under Integration click the [LDAP](#) link and you will be shown the settings in Figure 2.20. To integrate with the LDAP server, specify:

- the LDAP server's IP address as the Host IP address
- the LDAP Port for TCP communication (not the SSL port)
- any user's distinguished name as the User DN
- the Password for the user specified in the User DN field



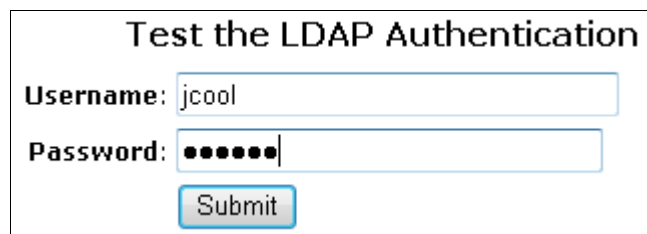
The screenshot shows a web form for LDAP integration. It has fields for "Host IP:" (192.168.1.115), "Port:" (3268), "Base DN:" (DC=RHUBCOM,DC=local), "User DN:" (CN=Joe Cool,OU=Snoopy,DC=PEAN), "Password:" (masked with dots), and "User Group Name:" (TurboMeetingUsers) with "(Optional)" text. A "Submit" button is at the bottom.

Figure 2.20 Enable LDAP integration

Only LDAP Version 3 is supported. No SSL encryption can be used for User DN and Password authentication. If a user with valid credentials fails to pass authentication by your LDAP server, check the following:

- Your LDAP configuration meets with the work conditions of this system.
- Your LDAP entries have the "distinguishedName" (DN) attribute filled with proper values. Empty values are not allowed. A Microsoft Active Directory server should automatically fill proper values for distinguishedName. To determine a distinguishedName for a user (i.e.: a User DN), use an LDAP browser like [JXplorer](#), or on Windows ADSI Edit (adsiedit.msc)

You can test whether individual users can be found for the given LDAP settings as shown in Figure 2.21. Enter the login name and password for a specific user. The resulting page will say either "LDAP authentication succeeds" or show a detailed trace of where the LDAP authentication failed.



The screenshot shows a web form titled "Test the LDAP Authentication". It contains two input fields: "Username:" with the value "jcool" and "Password:" with masked characters "••••••". Below the password field is a "Submit" button.

Figure 2.21 Test specific LDAP Users to insure correctness of LDAP settings

If you have an LDAP server with many thousands of users, or if only a small subset of your LDAP users are going to host meetings on the RHUB appliance, you can achieve faster LDAP user lookups by specifying multiple Base DN's. Taken together, these multiple Base DN's will likely have fewer users than your entire LDAP tree.

### 3. Configuring the Firewall

---

There are three ways to deploy your RHUB appliance:

1. Outside the Firewall
2. Inside the Firewall and Accessible by Users outside Firewall
3. Inside the Firewall and not Accessible by Users outside Firewall

Depending on the deployment, you may or may not need to configure your firewall.

#### 3.1. Behind Firewall and Accessible by Users outside Firewall

This deployment (Figure 3.1) is most popular and it is typically done by connecting RHUB appliance with the DMZ port of your router. You can also place the RHUB appliance anywhere on your LAN.

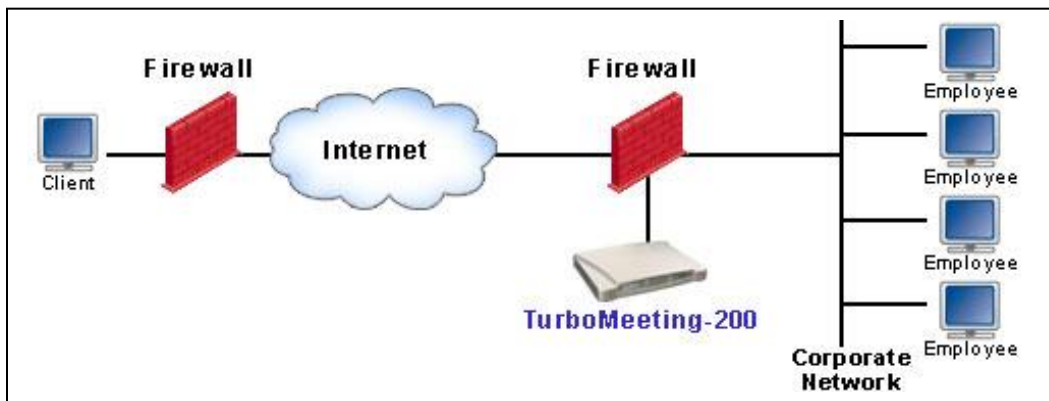


Figure 3.1 Inside Firewall and Accessible by Users outside Firewall

In order for external users to access your appliance, you need to open the inbound TCP ports: 80 and 443 and the TCP and UDP port 8889 on your firewall/router and forward the inbound TCP and UDP traffic on these ports to the corresponding ports of the local IP address of your RHUB appliance.

If you are using a SOHO or home router, opening inbound ports and doing port forwarding are fairly easy. For example, in a LinkSys router, you usually look for the "Applications" link. In a Belkin router, you look for the "Virtual Servers" link. After clicking the link, you will see a page similar to Figure 3.2. Fill in the two TCP ports (80 and 443) and the TCP and UDP port (8889) and your RHUB appliance local IP address. The firewall configuration is done.

In Figure 3.2, the "Private IP address" is the RHUB appliance's local IP address, which you define when you configure the meeting server IP settings; the "Inbound port" may be called "Source port"; the "Private port" may be called "Destination port". You can input anything in the "Description" field. Don't forget to check the "Enable" fields.

	Enable	Description	Inbound port	Type	Private IP address	Private port
1.	<input checked="" type="checkbox"/>	80	80 - 80	TCP	192.168.1.192	80 - 80
2.	<input checked="" type="checkbox"/>	443	443 - 443	TCP	192.168.1.192	443 - 443
3.	<input checked="" type="checkbox"/>	8889	8889 - 8889	Both	192.168.1.192	8889 - 8889

Figure 3.2 A sample of firewall configuration

This deployment gives you the maximum flexibility in terms of meeting access security control. With this deployment, you can host two types of meetings:

- Internal meetings that only users behind your firewall can join (including users in the Virtual Private Network, or VPN)  
Note: You can manually allow external users by specifying a list of IP addresses
- External meetings that anyone including attendees outside your firewall can join.

If you have difficulty in configuring port forwarding, please refer to the following URL for step-by-step guidance for your router:

[http://portforward.com/english/routers/port\\_forwarding/routerindex.htm](http://portforward.com/english/routers/port_forwarding/routerindex.htm)

On the page, find your router model or a model similar to yours. Click the link for your router. On the next page, click "Click here to skip this advertisement... ". Now it shows a long list of applications you can do port forwarding for. Just pick one application. Replace this application's port(s) with three different definitions for ports 80 and 443 using TCP and port 8889 using TCP and UDP.

### 3.2. Outside the Firewall

With this deployment (Figure 3.3), your RHUB appliance is completely outside your corporate firewall. There is no firewall configuration needed.

To configure the server settings (Figure 2.3) for this deployment, you will need to obtain from your Internet service provider (ISP) the IP address, subnet mask, default gateway and DNS settings. Input the IP address in the "Public IP Address" field and other IPs in the "Permanent IP Settings".

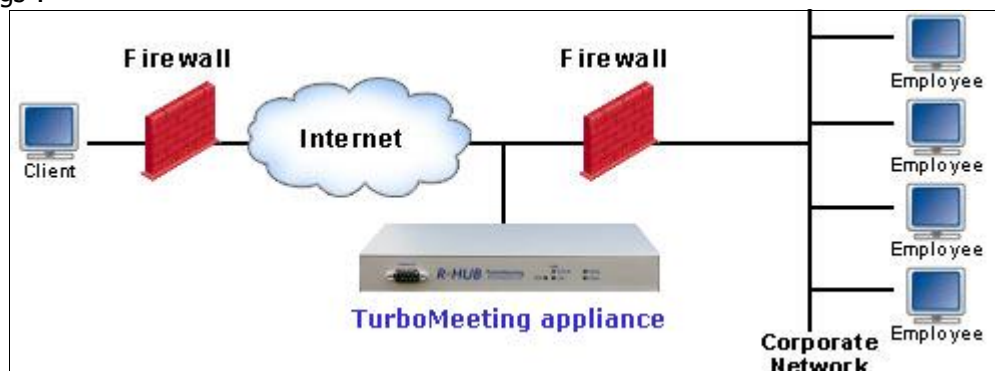


Figure 3.3 Deployment Outside the Firewall

### 3.3. Behind Firewall and Not Accessible by Users outside Firewall

This deployment (Figure 3.4) disallows users from connecting to the meeting server from the Internet outside your firewall and provides the maximum meeting access security. It will not allow any users outside your firewall (VPN) to join any meetings hosted on the server.

On the Server IP Settings configuration page (see Section 2.1), choose the option “No public IP address. This server is used only by internal users.” Then assign a static local IP, subnet mask, default gateway, and DNS servers for the meeting server (Figure 2.3).

You do not need to do any configuration on your firewall.

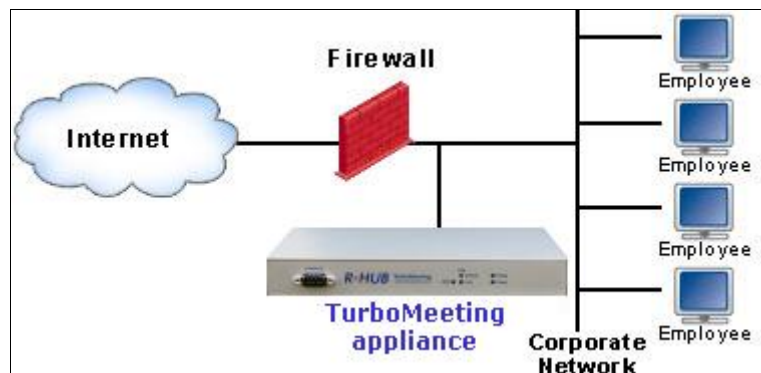


Figure 3.4 Inside Firewall and Not Accessible by Users outside Firewall



## 4. Manage Users

Login to the home page for your RHUB appliance and enter the management page shown in Figure 2.2. Under the User Management category, click the [Users](#) link. A list of users will display as shown below.

<a href="#">Add New User</a>						
First Name	Last Name	Email	Phone	Administrator	Status	Action
Admin		admin		Yes	Active	<a href="#">Edit</a>   <a href="#">Delete</a>
John	Doe	john@doe.com	213-564-6363	No	Active	<a href="#">Edit</a>   <a href="#">Delete</a>

Figure 4.1 List of Users

You can click the **Add New User** button to add a new user. Under the "Action" column, click the [Edit](#) link to edit a user profile or [Delete](#) link to delete a user profile from the system. Figure 4.2 below shows the page to create a user. You can define the meeting functions for each user.

### Create New User

**First Name**  \* (Required)

**Last Name**  \*

**Email Address**  \*

**Password**  \*

**Retype Password**  \*

**Phone**  \*

**User Group**

**Time Zone**

**Expiration**  Year  Month  Day

**Is Administrator** ☐ Yes ☒ No

**Meeting Privilege** (At least one meeting type is required)

☒ Meeting Type - Interactive Meeting

☒ Meeting Type - Seminar

☒ Meeting Type - Remote support

☒ Meeting Type - Remote access to my computer

☒ Send files

☒ Chat

☒ Record

☒ Multipoint video conferencing

Figure 4.2 Create a user profile

## 4.1. User Groups

User groups can be created to define the same set of meeting privileges, audio conference setting and promotional URLs for a group of users. Once a user group is created, users can be assigned to this user group. This makes it easier to assign similar meeting privileges to similar users.

User Groups definitions can also apply to user groups defined in LDAP. When creating a User Group using the following steps, insure that the user group name exactly matches the LDAP user group name.

To access user groups, login to the home page for your RHUB appliance and enter the management page shown in Figure 2.2. Under the User Management category, click the [User Group](#) link. A list of user groups will display as shown below.

List User Groups		
<a href="#">New User Group</a>		
User Group Name	Number of Users	Action
Executives	<a href="#">1</a>	<a href="#">Edit</a>
Sales	0	<a href="#">Delete</a>   <a href="#">Edit</a>

**Note:** In order to delete a user group, you need to remove all users from the group by setting the users to different user groups.

Figure 4.3 List of User Groups

You can click the **New User Group** button to add a new user group. Under the "Action" column, click the [Edit](#) link to edit a user group or [Delete](#) link to delete a user group from the system. To delete a user group, you must first remove all the users from that group. Figure 4.3 below shows the page to create a user. You can define the meeting functions for each user group.

## Create User Group

If the value of a field is empty, the system will use the corresponding system-wide value.

<b>Group Name</b>	<input type="text" value="Sales"/>	* (Required)
<b>Promotional URL, presented to attendees when meetings end</b>	<input type="text" value="http://www.YourCompany.com/sales"/>	
<b>Short URL to Join Meeting</b>	This URL is used to invite attendees verbally. By default, it is this server address. <input type="text" value="http://webmeeting.YourCompany.com/"/>	
<b>URL for Joining Interactive Meetings</b>	This URL is used to invite attendees via emails, which will be attached with meeting the id and password: "?id=xxx&password=yyy" <input type="text" value="http://webmeeting.YourCompany.com/"/>	
<b>URL for Joining Seminars</b>	This URL is used to invite attendees via emails, which will be attached with meeting the id and password: "id=xxx&password=yyy" <input type="text" value="http://webmeeting.YourCompany.com/"/>	
<b>Meeting Privilege</b> (At least one meeting type is required)	<input checked="" type="checkbox"/> Meeting Type - Interactive Meeting <input checked="" type="checkbox"/> Meeting Type - Seminar <input checked="" type="checkbox"/> Meeting Type - Remote support <input checked="" type="checkbox"/> Meeting Type - Remote access to my computer <input checked="" type="checkbox"/> Send files <input checked="" type="checkbox"/> Chat <input checked="" type="checkbox"/> Record <input checked="" type="checkbox"/> Multipoint video conferencing	
<b>Audio Conferencing Options</b>	<input type="radio"/> None <input type="radio"/> My audio conferencing number: <div style="border: 1px solid black; height: 20px; width: 100%; margin-bottom: 5px;"></div> My audio conferencing access code: <div style="border: 1px solid black; height: 20px; width: 100%; margin-bottom: 5px;"></div> <input type="checkbox"/> Use Meeting ID as the audio conference access code <input checked="" type="radio"/> RHUB integrated free audio conferencing service allowing the use of regular phones & computer microphones in the same conference.	
<div style="display: inline-block; border: 1px solid black; padding: 2px 10px; margin: 5px;">Submit</div> <div style="display: inline-block; border: 1px solid black; padding: 2px 10px; margin: 5px 10px;">Cancel</div>		

Figure 4.4 Create a user group

## 5. Start Meetings

After you complete the above configuration, you can start to host and invite people to join your meetings. Open your browser and type the IP address of the RHUB appliance into your browser. You should see the home page shown in Figure 1.1.

Click the "Host" button to host a meeting. The next page will ask you to accept a Java Applet. Accept it. TurboMeeting starts to run (Figure 5.1).

The Meeting Server Address in Figure 5.1 is your meeting server IP address. Type your email and password to start a meeting. The meeting control panel switches to the entry meeting control panel shown in Figure 5.2.

Tools | Help

Host Join Schedule

Email Address  
john@doe.com

Password  
\*\*\*\*\*

Meeting Server Address  
webmeeting.YourCompany.com

☒ Remember Me

Sign in

RHUB

Figure 5.1 Login to Start a Meeting

Tools | Help | Sign Out

Host Join Schedule

Scheduled Active

**List of scheduled meetings:**

1. Recurring (ID: 1243-9298) Seminar	
<a href="#">Start</a> <a href="#">Invite</a> <a href="#">Edit</a> <a href="#">Poll</a> <a href="#">Transfer</a>	
2. Recurring (ID: 1432-9240) <a href="#">Access</a> Remote Access	
<a href="#">Start</a> <a href="#">Invite</a> <a href="#">Edit</a> <a href="#">Poll</a> <a href="#">Transfer</a>	
3. 09/30/2013 02:00 PM (ID: 1706-0614) Interactive	
<a href="#">Start</a> <a href="#">Invite</a> <a href="#">Edit</a> <a href="#">Poll</a> <a href="#">Transfer</a>	

RHUB

Figure 5.2 Enter Meeting Control Panel

Click on the “Host” button as shown in Figure 5.2 and then select a meeting type. Your meeting starts (Figure 5.3).

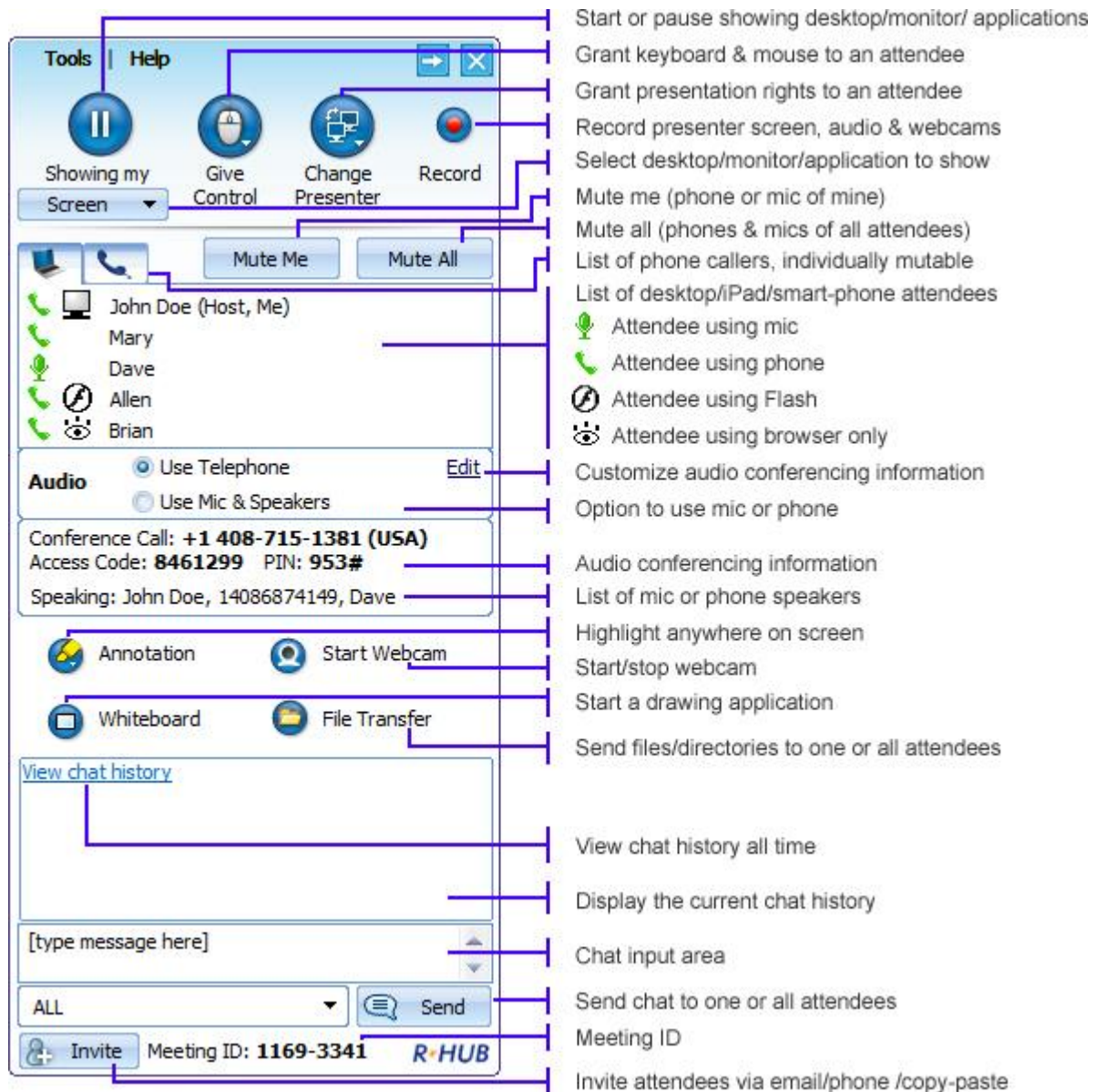


Figure 5.3 Main Meeting Control Panel

After the meeting starts, invite people to join your meeting by telling them the Meeting Server Address and the meeting ID shown on your meeting control panel. You can also click the “Invite” attendees button for more invitation details.

## 6. Reporting

---

In the left frame of the System Management page, click the [Report](#) link to use the Reporting feature. The reporting feature allows the Administrator to view details on all meetings that have taken place using a RHUB appliance. The report can be run for any specified dates and optionally for any set of users. The report data can also be downloaded into an Excel file.

Report - List of Meetings							
From	<input type="text" value="09/17/2009"/>		User	<input type="text" value="All Users"/>	<b>Total Meeting Time:</b> 48h 52m 40s (h: hour, m: minute, s: second)		
To	<input type="text" value="09/24/2009"/>		<input type="button" value="Get Report"/>		<a href="#">Download in Excel</a>		
Meeting ID	Host Name	Meeting Subject	Meeting Type	Number of Attendees	Start Time	Duration	IP Address
<a href="#">94283883</a>	John Doe	seminar	Seminar	2	09/23/2009 13:12:01	48m 44s	66.67.96.97
<a href="#">57899716</a>	Jane Doe		Interactive	2	09/22/2009 16:03:35	11h 31m 8s	66.92.15.4
<a href="#">22070986</a>	John Doe		Interactive	10	09/22/2009 16:03:16	11h 31m 32s	66.67.96.97
<a href="#">95843379</a>	Jane Doe		Interactive	56	09/21/2009 22:28:47	8h 36m 34s	66.92.15.4

Figure 6.1 Report of meeting activity

## 7. Reset Appliance

---

The following are two cases when you have to reset your appliance:

1. You forgot the administrator password
2. You move the appliance to a different network and you cannot access the appliance because you did not change the appliance IP settings for the new network while you could access the appliance in the previous network.

The RHUB appliance does three things during the reset:

1. It resets the system administrator account to the default one: "admin" as the email and "password" as the password. If you have multiple administrators, it only resets the first one's account.
2. It changes the IP settings to use DHCP.
3. It removes your own system home page URL so that you can easily access the appliance by a new IP address.

The reset does not affect any other data including user profiles, meeting logs, scheduled meetings, SSL certificate, audio integration setting, etc.

To reset the RHUB TM-200, TM-210, TM-260, TM-270, TM-510, TM-560, TS-300, or TW-100 appliances, you just push a pin into the reset button on the back and hold it for over 10 seconds until the "Ready" light turns off. After about 60 seconds when the "Ready" light turns on, you can access the appliance.

To reset the RHUB TM-600, TM-800, TM-1000, or TS-700 appliances, you need to connect it with your monitor, keyboard and mouse. The server runs in a Fedora Linux system. The default operating system login name is "turbomeeting" and the password is "password". After logging in, right click on the desktop and open a Terminal session. Type `./ResetTM`, which resets the appliance. Then open a browser and type "http://localhost" to access the TurboMeeting administration pages. Use the system default account: "admin" as the email and "password" as the password.

Refer to the Section 1.1 about how to access to your appliance after the reset.

## 8. License Upgrades: Additional Meeting Rooms and Users

To add meeting rooms or additional user licenses to your server, login as an administrator to your TurboMeeting System Management web page and click the [Request](#) link. Then fill in the number of additional meeting rooms and users and click Submit:

### License Request

<b>Current Number of Meeting Rooms</b>	50
<b>Current Number of Users</b>	200
<b>Number of Additional Meeting Rooms</b>	<input type="text" value="10"/>
<b>Number of Additional Users</b>	<input type="text" value="50"/>
	<input type="button" value="Submit"/>

Copy and paste the resulting page, below, into an e-mail and send it [sales@rhubcom.com](mailto:sales@rhubcom.com) :

<b>License Request</b>
<b>Model:</b> TM-1000
<b>Serial Number:</b> 112244
<b>Current Number of Meeting Rooms:</b> 50
<b>Current Number of Users:</b> 200
<b>Version:</b> 4.3 (build#: 3.0.19)
<b>Additional Meeting Rooms:</b> 10
<b>Additional Users:</b> 50
<b>Request Key:</b> ZxIFdhIqJilBWBuHfEJQODBgL24ZHEZaGh1qPQpDQxF0FVpL24ZHEZaGh1qPQpDQxF0FVpMRR%3D%3D
Please copy the entire license upgrade request message. If you purchased this TurboMeeting Appliance from a RHUB value-added reseller, please send this license upgrade request to them. If your reseller is not able to provide you adequate support, you may contact RHUB ( <a href="http://www.rhubcom.com">http://www.rhubcom.com</a> ) directly.

You will be sent an e-mail with a license request key. Login as an administrator to your TurboMeeting System Management web page and click the [Upgrade](#) link. Copy and paste the Request Key into the New License Key field and click Submit. Your license will be upgraded.

<b>Upgrade licenses</b>
<b>New License Key</b> <input type="text" value="S0s9FiIDJUKHQC8tQkhjWRZ6J3DBMD11ZAPQEBpDQxF0FVpMRRxFRwMuFUJcFjA%3D"/>
<input type="button" value="Submit"/>



## Support Contact

---

If you purchased the TurboMeeting Appliance from a RHUB value-added reseller, please contact them for support. If your reseller is not able to provide you adequate support, your reseller will contact us or you can contact us directly.

**RHUB Communications, Inc.**

4340 Stevens Creek Blvd.

Suite 282

San Jose, CA 95129

Tel: 408-899-2831 extension 2

Fax: 408-516-9612

[support@rhubcom.com](mailto:support@rhubcom.com)

<http://www.rhubcom.com>